

PRIVACY

The right to privacy is a bedrock principle of a free society and essential to today's economy. Yet, privacy protection is an ever-evolving field. To avoid harmful effects on competitive market forces, public policy on consumer privacy should reflect the following principles:

Policy should not create new “rights” that exist at the expense of the rights and resources of other private entities. Rights enumerated under the Bill of Rights of the United States Constitution are restrictions on government, not individuals or any other private entities. Therefore, technology companies should be free to regulate their own platforms and networks.

Neither public policy nor market forces are capable of creating perfect outcomes. Therefore, policy makers must weigh the tradeoffs of regulation. Policy makers need to recognize the problem of moral hazard that can arise when a certain activity comes to be viewed as carrying less risk than before. Designing or promoting policies as silver-bullet solutions can reduce consumer vigilance and encourage risky behavior.

They also need to account for regulatory barriers and regulatory capture. Regulation can reduce the number of choices for consumers in the marketplace. Less competition and less innovation ultimately harm consumers. It can also incentivize rent-seeking behavior through regulatory capture—lobbying to influence the writing of new regulations in ways that hobble new competitors.

The definition of privacy is subjective. The level of sufficient privacy for information varies because of many factors. Information privacy variables include: the content; to whom the information pertains and their preferences; with whom the information is shared; the medium by which the information is shared; the context in which the information is shared; how the shared information is used; how and the extent to which the information is retained.

The value of privacy is subjective. Implicit in the variable definition of privacy is the variable value that consumers derive from it. At a given level, standards of privacy may produce negative value. Examples of negative value include: lack of access to information that may produce better health and safety outcomes, lack of consumer data leading to wasteful allocation of resources, and reduced consumer choice.

Therefore, lawmakers should avoid setting privacy policy at the level of most concern. If 20 percent of people are extremely concerned about privacy, setting policy according to their preferences will harm the 80 percent who have a lower level of concern.

Market Alternatives and Potential Policies

- Encourage the proliferation of independent, third-party privacy ratings and certification.
- Reform antitrust law to allow for privacy coordination, knowledge-sharing, and standard-setting within industries.
- Create regulatory safe harbors to encourage good-faith efforts by tech companies to protect consumer privacy.
- Devise policy with an increased focus on the proper role of government in privacy protection: deterring fraud, enforcing contracts, and investigating and prosecuting malicious access to and use of information.